AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: s/Tiffany Edgmon 11-04-2024

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with google account "bornwicked420@gmail.com" that is stored at premises owned by Google LLC

Case No. M-24- 826-STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A," which is attached and incorporated by reference herein.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B," which is attached and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(2)	Distribution of Child Pornography

The application is based on these facts:

See the attached Affidavit of FBI Special Agent David Garrison, which is incorporated by reference herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

David Garrison, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: Nov 4, 2024

Judge's signature

City and state: Lone Wolf, OK [redacted]

SHON T. ERWIN, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David Garrison, Special Agent with the Federal Bureau of Investigation ("FBI"), Oklahoma City, Oklahoma, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI since June of 2005 and have been assigned to the Oklahoma City FBI Field Office since January of 2013. During that time, I have conducted a wide variety of investigations, including cases involving child pornography and sexual exploitation of children.

2. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a search warrant for information associated with a certain account, bornwicked420@gmail.com (herein after referred to as the **"SUBJECT ACCOUNT"**) that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. § 2252A.

4. This investigation, described more fully below, has revealed that an individual

knowingly utilized the BitTorrent peer-to-peer ("P2P") file-sharing network from 5309 NW 45th Street, Warr Acres, Oklahoma (herein after referred to as the RESIDENCE), to possess and distribute child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2), and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located on the **SUBJECT ACCOUNT**.

5. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

TERMS

6. Based on my training and experience, I use the following technical terms and definitions:

a. An Internet Protocol ("IP") address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, or long-term, IP addresses. Other computers have dynamic, or frequently changing, IP addresses.

b. Single-source download applies to a file that is downloaded from one IP address only. In P2P software, users often download different parts of the same file from many other users at once in an attempt to gain the file quicker. A single-source download comes from one user/IP address instead.

BACKGROUND ON P2P FILE SHARING

7. A growing phenomenon on the Internet is P2P file sharing. P2P file-sharing software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together.

8. To access the P2P networks, a user first obtains the P2P software from the Internet. This software is used exclusively for the purpose of sharing digital files. In general, P2P software allows the user to set up file(s) on his/her computer so that the files can be shared with others running compatible P2P software. In essence, a user allows his/her computer to be searched and accessed by other users of the network. If another user finds a file of interest on his/her computer, the other user may download that file. A user obtains files by opening the P2P software on his/her computer and conducting keyword searches of the P2P network. The P2P software then conducts a search of all computers connected to that network to determine whether any files matching the search term(s) are currently being shared by any other user on that network.

9. BitTorrent, one type of P2P software, sets up its searches by keywords, typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the actual files being shared, only the file referred to as a ".torrent" file. The user then selects one or more .torrent files from the results for download. The .torrent files contain instructions on how a user can download the file(s) referenced in the torrent. The download of file(s) referenced by the .torrent file is achieved using a BitTorrent client/program, through a direct connection between the computer requesting the file(s) and the computer(s) sharing the actual file(s) (not the .torrent file but the actual files referenced in the .torrent file, using any BitTorrent client/program).

10. For example, a person interested in obtaining images of child pornography would open

the BitTorrent website or program on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user then selects a .torrent from the results displayed. The .torrent file is the set of instructions a BitTorrent client/program needs to find the files referenced in the .torrent file. Once the .torrent file is downloaded, it is used by a BitTorrent client/program, previously downloaded and installed by the user, to download the actual files. The actual file(s) are downloaded directly from the computer or computers sharing the file(s). The download is achieved via the Internet. The downloaded file(s) are then downloaded/stored in an area previously designated by the user and/or the software. The downloaded files will remain until moved or deleted.

11. A P2P file transfer is assisted by reference to an IP address, which provides a unique location making it possible for data to be transferred between computers. The computer running the file sharing application, in this case a BitTorrent application, has an IP address assigned to it while it is on the Internet. BitTorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them.

12. Law enforcement officers using BitTorrent log the IP address which has sent the files or information regarding files being shared. Investigators can then search public records, such as ARIN, that are available on the Internet to determine the Internet service provider who has assigned that particular IP address. Based upon the IP address, investigators can obtain subscriber information from the Internet service provider. The subscriber information identifies the individual to whom the Internet service account is registered.

13. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user

may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers/sources. The advantage of this is that it speeds up the time it takes to download the file. However, software used by the FBI to download files from P2P networks will only download from a single source, via a direct connection (i.e., a single source download).

14. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person who shares child pornography files on a P2P network is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography.

15. Even though the P2P network links together computers from all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is specifically designed to only allow the download of files that have been selected. A user does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

BACKGROUND OF INVESTIGATION

16. This case originated on August 26, 2024, when law enforcement conducted an online undercover investigation to identify individuals possessing and sharing child pornography from July 25, 2024, August 5, 2024, and August 25, 2024, on the Internet using the BitTorrent P2P network. Law enforcement used a P2P file-sharing program that utilizes a single-source download process. Based upon my training and experience, I was familiar with P2P file-sharing, specifically the operation of the BitTorrent network. Law enforcement directed their focus to a computer using

IP address 68.97.174.205 because, on July 25, 2024, it was associated with a torrent file that referenced two files, at least one of which had been identified as a file of interest in child pornography investigations.

17. On August 5, 2024, between 6:17 p.m. and 6:30 p.m., Central Daylight Savings Time, law enforcement completed single-source downloads of approximately two files that the device using IP address 68.97.174.205 was making available for others to download on the BitTorrent network. Each of the files was downloaded directly from the device using IP address 68.97.174.205. Based upon my training and experience, I determined one of the files depicted children under the age of eighteen years engaged in lascivious exhibitions of the genitals, and sexually explicit conduct, that constitutes child pornography as defined by 18 U.S.C. § 2256. One of these files are described below:

a. Filename: pedomom.mp4
Description: A portion of this video depicts an adult female, with red fingernail polish, performing oral sex on a male toddler who is laying on his back. The female is wearing a mask that covers her face but exposes her eyes. The length of the video was 3 minutes and 53 seconds.

18. Between August 25, 2024, at approximately 8:12 p.m., and August 26, 2024, at approximately 7:51 a.m., Central Daylight Savings Time, law enforcement completed single-source downloads of approximately ten files that the device using IP address 68.97.174.205 was making available for others to download on the BitTorrent network. Each of the files was downloaded directly from the device using IP address 68.97.174.205. Based upon my training and experience, I determined several of these files depict children under the age of eighteen years engaged in lascivious exhibitions of the genitals, and sexually explicit conduct, that constitutes child pornography as defined by 18 U.S.C. § 2256. One of these files are described below:

a. Filename: 00303.mp4
Description: The video depicts a prepubescent female, with no clothes on

below her waist while sitting on a bed, performing oral sex on a male. She pulls her mouth away at one point and the male places his hand on the back of her head and holds her head while she continues to perform oral sex. Towards the end of the video, the prepubescent female puts her hands on her face and lays back onto the bed. The length of the video is 39 seconds.

19. Law enforcement determined that Cox Communications, Inc. was the Internet service provider for IP address 5309 NW 45th Street, Warr Acres, Oklahoma 73122. Pursuant to administrative subpoenas issued on August 7, 2024, Cox Communications, Inc. provided the following Internet subscriber information for the IP address 68.97.174.205 for the July 25 and August 5 downloads as described above[1]:

Name:	Dawn Weeks
Address:	5309 NW 45th Street, Warr Acres, Oklahoma 73122
Phone Numbers:	405-787-2105 405-808-6782

20. On September 17, 2024, a search warrant was executed at the RESIDENCE. During the course of the search and on-site preview of digital devices, no evidence of violations of 18 U.S.C. § 2252A was found. Additionally, during separate interviews, Dawn Weeks (Dawn) and her husband, Richard Weeks (Richard), disclosed individuals later identified as Brendon Shea Cooper (Cooper) and Katy Raeann Hale (Hale) resided at and near the RESIDENCE from approximately September of 2023 to July of 2024.

21. On September 17, 2024, I conducted an additional telephonic interview with Dawn who described how Cooper and Hale spent time at the RESIDENCE as indicated, but, following Dawn and Richard contracting Covid 19 around August 26-27, 2024, they have not spent as much time as previously. The last captured download of child pornography at the RESIDENCE was

[1] The results for the administrative subpoena to Cox Communications Inc. for the August 25-26, 2024 downloads is pending. It is anticipated the subscriber results will be the same as the previous subpoena returns.

August 26, 2024.

22. Due to an outstanding warrant for Cooper and drug paraphernalia charges, on September 17, 2024, Cooper and Hale were arrested by officers from the Warr Acres Police Department while sitting in a vehicle near the RESIDENCE.[2] At the time of their arrest, cell phones were in the control of or nearby both Cooper and Hale. Specifically, a black phone (black phone) was seized from the back passenger seat and a blue Motorola phone (Motorola) from the front passenger seat occupied by Hale. An additional TCL smart phone (TCL) was seized from Cooper's hand while sitting in the front driver's seat at the time of his arrest. All of the devices were collected by the Warr Acres Police Department and checked into their evidence control.

23. During the course of the search warrant at the RESIDENCE, the router was examined and its' log history was accessed revealing a number of MAC addresses[3] which utilized the router to gain access to the internet via the assigned IP address. On September 18, 2024, a search warrant was executed on the TCL, and the other devices, to determine if the MAC Addresses assigned to these devices were listed among the MAC Addresses displayed by the examined router. An examination of the black phone and Motorola revealed MAC Addresses that matched MAC Addresses found within the router log history, indicating they accessed the internet utilizing the assigned IP address and network located at the RESIDENCE. The MAC Address of the TCL did not match the listed MAC addresses contained within the RESIDENCE's router log history.

24. A subsequent search warrant was executed on the black phone and the Motorola. A forensic examination of the black phone did not reveal evidence related to the child pornography

[2] Officers with the Warr Acres Police Department located drug paraphernalia in the vehicle.
[3] A "MAC Address", or media access control address, is a unique identifier for a device on a network. It's a 12-digit hexadecimal number that's usually found on a device's network interface card.

downloads associated with the RESIDENCE. The examination of the Motorola revealed three images containing child pornography as defined by 18 U.S.C. § 2256. Additionally, one of the images appeared to be a still frame from the video, "pedomom.mp4", described in paragraph 17a of this affidavit. The referenced video was downloaded on August 5, 2024, utilizing BitTorrent software via the IP address assigned to the RESIDENCE.

25. A further examination of the Motorola revealed downloading of both utorrent and bittorrent client applications in February and April of 2024, respectively, which match the type of software and applications utilized by the individual(s) responsible for the child pornography downloads at the RESIDENCE.

26. Based on the evidence contained within the Motorola, a subsequent search was conducted on the TCL cell phone. Texts between Cooper and Hale (extracted from native messages from the TCL phone) from December 21, 2022 (during which they discussed sexual role playing) included the following:

> Cooper: I want to add something to the daddy and daughter Rp
>
> Hale: What's that baby
>
> Cooper: What big we add one of our girls to it not in real life but on here[4]
>
> Cooper: Don't judge
>
> Hale: Idk baby I don't want us to get caught and get in to trouble baby
>
> Cooper: We won't baby I promise
>
> Hale: But there is always that possibility though if the wrong person was to see
>
> Cooper: Delete once you are done baby
>
> Hale: As we we're doing it on here or our phone baby

[4] Hale has three prepubescent girls from a previous relationship.

Cooper: No one will see baby unless we just do it in real life which would be hot as well lol

Hale: No we ain't doing it in real life baby what would make you think I would feel ok with that. How about we just make up a random girls name instead baby

27. During a text exchange on January 9, 2023, Cooper and Hale discussed incorporating one of Hale's juvenile daughters in their sexual activities. At one point of the exchange, Cooper stated, "Ok, so JANE DOE[5] has caught me naked with you and she has talked to me about it but she does want to start playing with us in bed and she wants to be played with too I have told her if that ever happened and she says anything to anyone me and you would get in trouble but she swears up and down she won't and I believe her so was going to see if she could sleep with us a night or two a week and us three have fun and see if we like it but I don't want you mad at me or her because I love you and respect you but I think it will be fun and I kinda want to does that make me a bad person baby"

28. A series of emails (ranging from December 8, 2022 to January 25, 2023) from notification@facebookmail.com (titled "Facebook Groups") to both an @groups.facebook.com Brendon Cooper email address and the **SUBJECT ACCOUNT** verified membership in various Facebook Groups for Cooper's Facebook account[6]. The groups included: "Littles and Abdi Play Space"[7], "Incest Love", "DDLG centre"[8], "Mommies and Littles/Middles Safe Place 18+", "TEENS CLUB (joking) (13-21)", "CUTE KIDS AROUND THE WORLD", and "Secret Room".[9] The **SUBJECT**

[5] Hale's second oldest daughter who was nine years old at the time of this text exchange.
[6] A subpoena to Facebook for subscriber information for the referenced account, 100088501780416, was returned on Nov. 1, 2024 listing Brendon Cooper as the subscriber.
[7] This group caters to individuals who have fetishes involving "Adult Baby/Diaper Lover" and "Daddy Dom/Little Girl" roleplays.
[8] DDLG means "Daddy Dom/Little Girl"
[9] Facebook groups set to "private" or 'secret" allow only members to access and see the content.

ACCOUNT was used by Cooper to register his Facebook account.[10]

29. On December 22, 2022, Cooper received a message on his Facebook account from a Facebook user for the group "Little café DDLG, MDLG, DDLB, MDLB, CG, PETS"[11]: "Anybody have discord and want to join a group for littles[12]".

30. Through my training and experience, it is common for individuals engaged in the downloading and storing of child pornography to move or transfer the material from one digital device to another, or from social media/instant messaging platforms to digital devices for ease of access, to include cloud or online storage websites. Due to Cooper using the **SUBJECT ACCOUNT** to register his Facebook account and the nature and substance of the communications and group activities with which Cooper was engaged on his Facebook account, I believe it is reasonable to believe Cooper has used the **SUBJECT ACCOUNT** to further engage in violations of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2),

BACKGROUND CONCERNING GOOGLE[13]

31. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service

[10] The referenced Nov 1, 2024, Facebook subpoena (footnote 6) listed the SUBJECT ACCOUNT as the "verified primary" email address.
[11] MDLG means "Mommy Dom/Little Girl", DDLB means "Daddy Dom/Little Boy", MDLB means "Mommy Dom/Little Boy", CG means "Caregiver" usually of someone acting as a "Little" or juvenile, PET can mean a submissive in a Dom/Sub relationship.
[12] Littles is a term used by individuals acting or conversing at an age younger than they truly are, usually as a minor.
[13] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

32. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

33. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

34. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

35. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

36. Google also provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video

communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

37. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

38. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

39. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a

communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

40. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. The subscriber information, saved photos, documents, messages, and emails associated with the **SUBJECT ACCOUNT** will help establish who owns the **SUBJECT ACCOUNT** and determine to what extent the **SUBJECT ACCOUNT** has been engaged in violations of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2).

41. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. For example, images of child pornography may be stored within the Google Photos service associated with the **SUBJECT ACCOUNT**. Further, data from the **SUBJECT ACCOUNT's** Chrome history, "My Activity" feature, and messaging services could provide evidence of the suspect's acquisition and subsequent distribution of child pornography.

42. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs,

documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

44. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of downloading and possessing child pornography. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of other instrumentalities of the crimes under investigation.

45. Therefore, Google's servers are likely to contain stored electronic communications and information concerning the subscriber of the **SUBJECT ACCOUNT** and his or her use of Google services. In my training and experience, such information may constitute evidence of the

crimes under investigation including information that can be used to identify the account's user or users.

ADDITIONAL CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

46. The following indicates characteristics of child pornography collectors that I have learned through training, working multiple investigations involving child pornography, and from other law enforcement officers with a background in child pornography investigations:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer to peer, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual

activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location.

CONCLUSION

47. Based on the above information, and my training and experience, the user of the **SUBJECT ACCOUNT** is engaging in behavior indicative of an individual who has a sexual attraction to children and there is probable cause to believe that the foregoing laws have been violated, and that the property, evidence, fruits, and instrumentalities of these offenses are located on the **SUBJECT ACCOUNT.**

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google. Because the warrant will be served on Google, who will then compile the

requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

49. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States" with "jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

50. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the **SUBJECT ACCOUNT**, described in Attachment A, authorizing the seizure of the items described in Attachment B to this Affidavit.

David Garrison
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 4th day of November 2024.

Shon T. Erwin
SHON T. ERWIN
United States Magistrate Judge

ATTACHMENT A

This warrant applies to information associated with bornwicked420@gmail.com (**SUBJECT ACCOUNT**), which are stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The **SUBJECT ACCOUNT** was preserved with Google on 10/24/2024.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose to the government for the **SUBJECT ACCOUNT** listed in Attachment A the following information, from December 1, 2022, to the present:

a. All business records and subscriber information, in any form kept, pertaining to the **SUBJECT ACCOUNT**, including:
   1. Names (including subscriber names, user names, and screen names);
   2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
   3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
   4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
   5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers;
   6. Length of service (including start date and creation IP) and types of service utilized;
   7. Means and source of payment (including any credit card or bank account number); and
   8. Change history.

b. All device information associated with the **SUBJECT ACCOUNT**, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the **SUBJECT ACCOUNT**, including, for all Google services, the date, time, length, and method

of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;

d. The contents of all media associated with the **SUBJECT ACCOUNT** in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; all associated logs of each record, including the creation and change history, access logs, and IP addresses; and any settings that may indicate that images or other data were automatically uploaded from the synced device to Google Photos;

e. The contents of all emails associated with the **SUBJECT ACCOUNT**, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

f. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history; and

g. The contents of all records associated with the **SUBJECT ACCOUNT** in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

h. The contents of all text, audio, and video messages associated with the **SUBJECT ACCOUNT**, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

Google is hereby ordered to disclose the above information to the government within 14 days of

issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A), Distribution of Child Pornography, and 18 U.S.C. 2252A(a)(5)(B), Possession of Child Pornography, those violations involving the unknown suspect and occurring from December 1, 2022, to the present, including, for the **SUBJECT ACCOUNT** listed on Attachment A, information pertaining to the following matters:

a. Evidence of the possession, access with intent to view, and distribution of images depicting children engaged in sexually explicit conduct.

b. Evidence indicating how and when the **SUBJECT ACCOUNT** was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the **SUBJECT ACCOUNT** owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the **SUBJECT ACCOUNT**, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Affiant may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.